UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

FILED
14 APR 21 AM 11:40
MICHAEL R. MERZ
UNITED STATES
MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Generic brand desktop computer with the number 02104159 I-501 ATX2 on the back and two VHS tapes, both located in the Evidence Control Room of the FBI

Case No. 3:14 mj - 155
MICHAEL R. MERZ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:
- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C	

The application is based on these facts:
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: __________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R Kinzig
Applicant's signature

Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: April 21, 2014

Judge's signature

City and state: Dayton, Ohio

Michael R. Merz, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

(1) Generic brand desktop computer with the number 02104159 I-501 ATX2 on the back, previously located in a maintenance closet at the Hampton Inn at 8960 Mall Ring Road in Dayton, Ohio; and (2) two VHS tapes with no labels; both of which are currently located in the Evidence Control Room of the Federal Bureau of Investigation, 7747 Clyo Road, Centerville, Ohio, 45459.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of Title 18, United States Code, **Sections 2252** and **2252A** (advertising, promoting, presenting, distributing, or soliciting through interstate or foreign commerce by any means, child pornography), including but not limited to the following:

1. Evidence of the utilization of the email addresses daddyjohn777@gmail.com, smoothies555@hushmail.com, and any other email accounts utilized to send or receive child pornography.

2. Evidence of utilization of any Internet websites or computer software or programs to send or receive child pornography.

3. Evidence of utilization of any cloud storage services.

4. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

5. Documents and records regarding the ownership and/or possession of the computer media.

6. Any and all images or videos depicting child pornography and/or child erotica.

7. Any and all visual depictions of minors.

8. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

9. Any books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by

computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

11. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

ATTACHMENT C

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)	Receipt and Distribution of Child Pornography

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
Western Division

FILED
14 APR 21 AM 11:40
MICHAEL R. MERZ
UNITED STATES
MAGISTRATE JUDGE

IN THE MATTER OF THE SEARCH OF:)
Generic brand desktop computer with the) Crim. No. 3:14 MJ 155
number 02104159 I-501 ATX2 on the back)
and two VHS tapes, both located in the) **FILED UNDER SEAL** MICHAEL R. MERZ
Evidence Control Room of the FBI)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media.
2. Along with other agents and task force officers of the Federal Bureau of Investigation, I am currently involved in an investigation of the possession, distribution, and receipt of child pornography by EUGENE ROBERTS (hereinafter "ROBERTS"). This Affidavit is submitted in support of an Application for a search warrant for a **generic brand desktop computer with the number 02104159 I-501 ATX2 on the back** and **two VHS tapes** (hereinafter collectively referred to as "**SUBJECT COMPUTER MEDIA**") for evidence of violations of 18 U.S.C. § 2252 and 2252A. **SUBJECT COMPUTER MEDIA** is more fully described in Attachment A hereto. The purpose of this Application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography; and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography through interstate commerce. The items to be searched for and seized are described more particularly in Attachment B hereto.
3. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have heresay knowledge.
4. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of the **SUBJECT COMPUTER MEDIA**.

5. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, are present at the **SUBJECT COMPUTER MEDIA**.

PERTINENT FEDERAL CRIMINAL STATUTES

6. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
7. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
8. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly possess with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
9. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
10. For purposes of these statutes, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) as:

    a. "Actual or simulated –
        i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

ii. Bestiality;
iii. Masturbation;
iv. Sadistic or masochistic abuse; or
v. Lascivious exhibition of genitals or pubic area of any person."

DEFINITIONS

11. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. "**Internet Service Providers**" or "**ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An **Internet Protocol address**, also referred to as an **IP address**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. A network "**server**," also referred to as a "**host**," is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

h. A **client** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

i. "**Domain Name**" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (*i.e.,* 149.101.1.32), to enable the follow of traffic across the Internet.

j. "**Log Files**" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

k. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a.

"resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

l. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

n. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

12. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives, including ICE's "Operation Emissary" and the FBI's "Ranchi message board" investigation. For example, in the "Ranchi" investigation a national take-down occurred during the week of March 1, 2007. Approximately 83 subjects were contacted, 28 by court-authorized search warrants and 55 by "knock and talks." Of the 83 contacts, 46 individuals (or 55%) confessed to accessing the Ranchi message board and/or downloading child pornography from Ranchi. Multiple other new cases were opened without confessions based on strong evidence obtained during the Ranchi search warrants and knock-and-talks.

USE OF COMPUTERS AND THE INTERNET WITH CHILD PORNOGRAPHY

13. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

a. **Production**: Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.,* lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

b. **Communication**. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

c. **Distribution**. Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

d. **Storage**. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

14. As previously stated, the investigation has determined that one or more computers are located at the **SUBJECT PREMISES**, and such computer(s) is/are being used as an instrumentality in the course of, and in furtherance of, the transmission and possession of child pornography as described above. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form. This includes computer hard-drives, disks, CDs and other similar electronic storage devices.

15. As indicated above, computer hardware is used to save copies of files and communications, while printers are used to make paper copies of same. Programs loaded on the drives are the means by which the computer can send, print and save those files and communications. Finally, password and security devices are often used to restrict access to or hide computer software, documentation or data. Each of these parts of the computer is thus integrated into the entire operation of a computer. In order to best evaluate the evidence, the computers—and all of the related computer equipment described above—should be available to a computer investigator/analyst.

Forensic Imaging

16. An important step that is ordinarily part of an expert's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

17. Special software, methodology and equipment are used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, which is an incredibly large number that is much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

18. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and

custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

19. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last modified; when was it last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.

20. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The contents of Adobe ".pdf" files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner–ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

21. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

22. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

Persistence of Digital Evidence

23. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is "deleted" by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.

24. Typically, computer forensics focuses on at least three categories of data. These are: 1) **active data** – such as current files on the computer, still visible in file directories and available to the software applications loaded on the computer; 2) **latent data** – such as deleted files and other data that resides on a computer's hard drive and other electronic media in areas available for data storage, but which are usually inaccessible without the use of specialized forensic tools and techniques; and 3) archival data – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

25. **Active data** includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.

26. **Latent data** includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.

27. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

Conclusion Regarding Forensic Analysis Procedures

28. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location the computers and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the

premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

29. Therefore, it is respectfully requested that the warrant sought by this application authorize the search and seizure for all "computer hardware," "computer software" and documents, which are more fully set-out and explained above, and further authorize a full physical and forensic examination of the seized items at a secure location.

BACKGROUND ON CLOUD STORAGE AND MEDIA FIRE

30. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:

a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

b. "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

i. "Infrastructure as a Service" (IaaS) allows a consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

ii. "Platform as a Service" (PaaS) allows a consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

iii. "Software as a Service" (SaaS) allows a consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

c. "Cloud Service Provider" (CSP) is the entity that offers cloud computing services. CSP's offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP's maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP's reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long-term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a "remote computing service." CSP's may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

d. "Virtual Machine" (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred.

A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

31. MediaFire, a company headquartered in Shenandoah, Texas, is one example of a CSP. Media Fire advertises the following about its services on its website (www.mediafire.com):

a. "MediaFire stores all your media and makes it available to you anytime you want it, anywhere you go, on any device you have."
b. "Share your media *as media*. Your photos, videos, songs, and documents are more than just files. On MediaFire you can share, view, and listen to over 200 different file formats – all right in your web browser or mobile device."
c. "Life is better when shared with friends. Collaborate on projects, share folders and files, and control who can edit and who can view. Invite friends to connect through Facebook, Google, Twitter, or via email."
d. "With up to 50GB of free space, you can use MediaFire to backup all your important files—and even your not-so-important ones too. Your files are used securely and privately and are always available to you."

BACKGROUND OF INVESTIGATION

32. Since August 2013, agents and task force officers of the Federal Bureau of Investigation have investigated JOHN WAYNE SOPER for child pornography offenses. SOPER was indicted in January 2014 in the United States District Court for the Eastern District of Michigan for one count of child exploitation enterprise (in violation of 18 U.S.C §2252A(g)), ten counts of production of child pornography (in violation of 18 U.S.C §2251(a)), one count of transportation of child pornography (in violation of 18 U.S.C. §2252A(a)(1)), one count of receipt of child pornography (in violation of 18 U.S.C §2252A(a)(2)), and one count of possession of child pornography (in violation of 18 U.S.C §2252A(a)(5)(B)).

33. As part of the investigation of SOPER, agents identified that he utilized the email account mygirlsrsweetest@gmail.com to send and receive child pornography. On or around September 24, 2013, a search warrant was authorized by the United States District Court for the Eastern District of Michigan for the email account mygirlsrsweetest@gmail.com. Based on records received from Google, Inc. in response to the search warrant, agents identified that one of the individuals with whom SOPER traded child pornography (among numerous others) was the user of the email account daddyjohn777@gmail.com. The display name[1] for this email account was "John Farris".

---

1 The display name for an email account is a common name that automatically accompanies an email address and is displayed to the recipient. The display name is utilized to help identify the sender's identity to the recipient. Display names can be set by the email account user through the account's Configuration settings. For most email accounts, the display name appears in the sender line of the email followed by the email address surrounded in angled brackets. For example, if "John Doe" is the display name for the email account jdoe@example.com, the sender line of the email account will appear as "John Doe <jdoe@example.com>" to the recipient.

34. An additional search warrant was authorized by the United States District Court for the Eastern District of Michigan for the email account daddyjohn777@gmail.com on or around November 18, 2013. Google, Inc. provided records in response to this search warrant for the time periods of February 11, 2013 to April 1, 2013 and September 19, 2013 to November 18, 2013. Agents are still awaiting a response from Google, Inc. regarding any records available for the time period of April 2, 2013 to September 18, 2013.

35. Subscriber information for the daddyjohn777@gmail.com account indicates that the account was created on or about November 3, 2012. The user identified his name as being "John Farris" when opening the account. Review of the email contents for the account indicated that the account was used nearly exclusively to send and receive child pornography and to communicate with other individuals about sexual interests in children. In total, more than 100 email messages were sent to or from the account in which files depicting child pornography were attached. These messages were exchanged with at least 20 other email accounts.

36. Based on the contents and context of many of the messages, it appeared that the user of the daddyjohn777@gmail.com account met some of the individuals with whom he traded child pornography on a publicly available file-sharing website that will be referred to for purposes of this Affidavit as "Website A". Based on my training and experience, I know that Website A is commonly used to facilitate the advertisement, dissemination, and production of child pornography and to establish trading contacts among users.

37. Many of the email messages recovered from the account indicated that the user of the daddyjohn777@gmail.com account engaged in a "quid pro quo" trading relationship with other users – i.e., that after sending files depicting child pornography to other users, the account user expected to receive files in return. Two examples of this trading relationship are as follows:

Example 1:

a. **Email dated November 17, 2013, from daddyjohn777@gmail.com to george_smithton@yahoo.com with a subject line of "New"**: The message contained within this email stated, "Hope these aren't too hardcore for you." Attached to the message were three video files depicting child pornography (as defined by 18 U.S.C. § 2256). One of these files is described as follows:

omg 03.avi: The file depicts a video that is approximately three minutes and 11 seconds in duration. The video begins by showing a young, pre-pubescent white female child lying on her back. She is wearing a diaper, green socks, and a dark-colored mask. An adult white male, who is only depicted from the waist down, removes his pants and kisses the female child on her mouth. He then pulls aside her diaper, engages in oral sex with her, and fondles her vagina and buttocks. The adult male then puts his penis into the child's mouth so she can perform oral sex on him. The child is heard crying and gagging throughout the video.

b. **Email dated November 17, 2013 from george_smithton@yahoo.com to daddyjohn777 with a subject line of "Re: New"**: This email was a response to the email noted above. The message contained within the email stated, "Not at all,nothing is to hardcore, love them and these I'm sending very much ,, I have,omg 03,,and omg 05,and did have omg 02,but have it now again, thanks very much!!". Attached to the message were three video files depicting child pornography (as defined by 18 U.S.C. § 2256). One of these files is described as follows:

> **(-Jho-) 6Yo Tiny Tessa (2) Ass Fucked Screaming 2008.wmv**: The file depicts a video that is approximately 18 seconds in duration. A pre-pubescent white female child is lying on her back on a white cover with her legs spread apart, exposing her vagina to the camera. She is only captured from the stomach down, and she appears to be completely naked. The white male inserts his penis repeatedly into the female child's buttocks, anally penetrating the child. The female child is heard crying.

Example 2:

c. **Email dated March 30, 2013 from putitinyrmouth50@gmail.com to daddyjohn777@gmail.com with no subject line**: There was no message contained within the email. Attached to the email were five image files depicting child pornography (as defined by 18 U.S.C. § 2256). One of these files is described as follows:

> **PTHC Pedo NEW Childporn Private Daughter Torpedo Ranchi Lolita - Melinda 2406.jpg:** The image depicts a young pre-pubescent white female child lying on her back on a blue cover. She is only captured from the waist down, and she appears to be completely naked. The penis of a white male is inserted into the female child's buttocks, anally penetrating the child.

d. **Email dated March 30, 2013 from daddyjohn777@gmail.com to putitinyrmouth50@gmail.com with the subject line "Re:":** This email was a response to the email noted above. The message contained within the email stated: "Also, I love black men with little white girls and very young black girls." Attached to the email were eight image files, seven of which depict child pornography (as defined by 18 U.S.C. § 2256). One of these files is described as follows:

> **IMG_3770.JPG**: The image depicts a white female child with brown hair leaning over a white male, who is only captured from the groin area. The white male has a red bow wrapped around his penis. The white male's penis is in the mouth of the female child.

38. In a number of the email messages, the user of the daddyjohn777@gmail.com account told other individuals that he maintained a large collection of child pornography, and he discussed his preference in the ages of the children. Three examples of such emails are as follows:

a. On October 24, 2013, the daddyjohn777@gmail.com account user received approximately 48 files (at least 34 of which depicted child pornography, as defined by 18 U.S.C §2256) from an individual utilizing the email address testme1025@yahoo.com. The daddyjohn777@gmail.com account user responded to the message by stating: "I want these 3. I LOVE sleeping pics and vids. Reminds me of my fun with my daughter from age 6 – 13.. mmmmmmm". The email from daddyjohn777@gmail.com had approximately 43 files (at least 27 of which depicted child pornography, as defined by 18 U.S.C §2256) attached to the message.

b. On March 27, 2013, the daddyjohn777@gmail.com account user told an individual utilizing the email address stewiejr2012@gmail.com: "I always loved bath time with my girls. I would help them til ages 10 and 11. They were two of the hottest girls I've ever seen.

c. On August 31, 2013, the daddyjohn777@gmail.com account user told mygirlsrsweetest@gmail.com (SOPER's email address): "I forgot to tell you. I have a beautiful granddaughter that just turned 2, a few weeks ago. She has a very, very tasty pussy."[2]

42. A number of the email messages recovered from the daddyjohn777@gmail.com account indicated that this account user as well as others with whom he communicated utilized various cloud storage devices to store some of their files depicting child pornography – including Dropbox, MediaFire, and a service called "MyDrive". In some cases, the daddyjohn777@gmail.com account user and the others with whom he communicated provided each other with their user names and passwords to their accounts so they could share their child pornography files. For example:

a. On November 16, 2013, the daddyjohn777@gmail.com account user sent an email message to george_smithton@yahoo.com (an individual with whom the daddyjohn777@gmail.com account user had exchanged files depicting child pornography on at least 12 other occasions). In this email message, the daddyjohn777@gmail.com account user stated: "Go to mediafire.com Log in with my username and pw. You will access all my videos on there, and you can upload some for me also. daddyjohn777@gmail.com pw = qpqpwo1234 I'm sure you will blow some great loads on them. LOL"

b. On November 15, 2013, the daddyjohn777@gmail.com account user sent an email message to mimixzm@yahoo.com containing approximately four files depicting child pornography (as defined by 18 U.S.C. §2256). In this email, the daddyjohn777@gmail.com account user stated: "Here's a little taste to see if you are a real trader. And yes, I use mediafire for large vids."

c. On March 27, 2013, the daddyjohn777@gmail.com account user received an email message from vinhnhimc@yahoo.com (an individual with whom the daddyjohn777@gmail.com account user had exchanged files depicting child pornography on at least 16 other occasions). The vinhnhimc@yahoo.com account

2 It should be noted that this email message was recovered from the records provided by Google for the mygirlsrsweetest@gmail.com account. All other email messages referenced in the Affidavit were recovered from the records provided by Google for the daddyjohn777@gmail.com account.

user stated: "Send you, I love 3-12yo vids & pics, :D". The daddyjohn777@gmail.com account user responded to this email with a message stating: "Go to my "mydrive" account. username is daddyjohn, pw is pussy2. Enjoy"

d. On February 28, 2013, the daddyjohn777@gmail.com account user received an email message from teendreamz77@gmail.com (an individual with whom the daddyjohn777@gmail.com account user had exchanged files depicting child pornography on at least two other occasions). In this email, the teendreamz77@gmail.com account user stated: "hey john! i would like it if you fill your mydrive up to 2 GB, like I did last time thnx!"

43. In March 2014, records were received from MediaFire regarding the user account for daddyjohn777@gmail.com. Records identified that this account was created on or about July 28, 2013, utilizing an IP address of 108.81.130.222. Records further identified that over 90 files with file names indicative of child pornography had been uploaded to the daddyjohn777@gmail.com account during the approximate time period of January 2014 to February 2014. Records indicated that approximately eight of the files were still in the user's drive, while the remaining had been deleted. Furthermore, approximately 55 of the files were uploaded by the user utilizing an IP address of 108.81.130.222. Examples of some of these files are as follows:

a. **babyj-fucked to Pieces-1.wm**: Uploaded on February 5, 2014
b. **playing with a hot black 9yo.mp4**: Uploaded on February 6, 2014
c. **man fucks his 12yo stepson.avi**: Uploaded on January 19, 2014 (but subsequently deleted)
d. **dad fucks son 7 while sleeping.mpf**: Uploaded on January 19, 2014 (but subsequently deleted)

44. Utilizing a law enforcement tool, a report was generated that identified user information from Website A for the account with the user ID of "daddyjohn". This report identified that the account was registered on or around November 23, 2012. The user identified a primary and secondary email address of daddyjohn777@gmail.com. The IP address utilized to register the account was 108.81.130.222 (the same address utilized on the daddyjohn777@gmail.com MediaFire account, as noted above).

45. Google, Inc. provided a log of IP addresses that were utilized to log into and log out of the daddyjohn777@gmail.com account. The logs appeared to contain IP addresses for a dynamic account. However, the IP address of 108.81.130.222 (the address utilized on the MediaFire account and to register on Website A) was utilized on one occasion to log into and out of the email account. The log further indicated that service for the email account was ended on or around November 28, 2013.

46. AT&T Internet Services, who is the service provider for the IP address of 108.81.130.222, provided records in response to an administrative subpoena regarding the subscriber of the account. The records identified that on the date and time that the IP address was utilized to register the Website A account, it was subscribed to ROBERTS. As of at least March 16, 2013, the service and billing addresses for the account were 2949 Kingston Avenue, Dayton, Ohio. According to AT&T's records, the account was

established on January 9, 2012, and was open/active as of the date the records were provided (on or around March 19, 2014). The records also identified that the preferred email address for ROBERTS was geno.roberts@yahoo.com, and that his cellular telephone number was 937-699-0597.

47. An additional administrative subpoena was serviced to AT&T Internet Services for a sample of four suspected dynamic IP addresses utilized to access the daddyjohn777@gmail.com account on the following dates: May 25, 2013; November 3, 2013; November 17, 2013; and November 18, 2013. Based on records received from AT&T, the four noted IP addresses were provisioned accounts from the 108.81.130.222 account, and as such, were subscribed to ROBERTS at 2949 Kingston Avenue, Dayton, Ohio. The records indicated that the account for the 108.81.130.222 IP address continued to be open as of March 30, 2013.

48. On November 2, 2013, the daddyjohn777@gmail.com account user sent an email to geno.roberts@yahoo.com. Attached to this message were five PDF files containing receipts or payment confirmations for payments made to Time Warner Cable. The payments appeared to be for cable bills. One of the files identified that the payment was made utilizing a credit card with an account name of "Eugene Roberts".

49. Based on records from the Ohio Bureau of Motor Vehicles, ROBERTS utilized the address of 2949 Kingston Avenue, Dayton, Ohio, on his current Ohio driver's license. He also utilized this address when registering at least two motor vehicles. According to records from the Dayton Police Department, officers were dispatched to the residence at 2949 Kingston Avenue, Dayton, Ohio, on two occasions in January 2012 and June 2013. On both occasions, ROBERTS was present and identified that he resided at the residence. In January 2012, he identified that his aunt also lived at the house in the basement. In June 2013, ROBERTS identified that his ex-girlfriend and the ex-girlfriend's daughter had been temporarily staying at his house for the past month.

50. Cricket Wireless was identified as the service provider for the cellular telephone number 937-699-0597 (the contact telephone number noted on AT&T Internet Services' records for the 198.81.130.222 IP address). Records received from Neustar on behalf of Cricket Wireless identified that the telephone number 937-699-0597 was subscribed to ROBERTS, with a customer address of 2949 Kingston Avenue, Dayton, Ohio.

51. Based on my training and experience, I know that it is common for individuals to utilize multiple email accounts. Individuals may use different accounts for different purposes (i.e., one account for work purposes and another account for personal emails) or use different accounts for use on different devices (i.e., one account for use on a home computer and one account for use on a telephone). It is common for individuals to email files from one email account to another in order to transfer the files to different computer devices.

52. Again based on my training and experience, I know that child sex offenders who communicate with victims and other offenders via email commonly utilize fictitious names and / or multiple accounts. Similarly, such child sex offenders may utilize one account for general communications and other accounts for communications with victims and other offenders. Furthermore, such individuals frequently change their email account names. The use of fictitious names and multiple accounts and the practice of changing accounts on a regular basis are all means to conceal their identities and criminal activities.

53. I also know, based on my training and experience, that individuals involved in child pornography offenses are increasingly utilizing cloud computing. Individuals with large collections of child pornography may utilize cloud computing as a means to store their files after their hard drives become full. In addition, individuals utilize cloud computing as a means to conceal their files from others in the residence and/or from law enforcement.

54. On April 2, 2014, a search warrant was authorized by the United States District Court for the Southern District of Ohio for the residence at 2949 Kingston Avenue, Dayton, Ohio. Agents and officers of the Federal Bureau of Investigation and the Dayton Police Department executed this warrant on the morning of April 3, 2014. Present when agents and officers arrived were ROBERTS, four adult females, and a two-year old child.

55. During the execution of the warrant, ROBERTS consented to be interviewed after being advised of his Miranda rights. In summary, ROBERTS provided the following information:

a. ROBERTS confirmed that he resided at 2949 Kingston Avenue, Dayton, Ohio, along with three of the adult females (one of whom he considered to be his step-daughter, although he was never married to the woman's mother) and the two-year old child (who he considered to be his granddaughter).

b. ROBERTS confirmed that he was the user of the daddyjohn777@gmail.com and geno.roberts@yahoo.com email addresses.

c. Although he first denied any involvement in viewing or accessing child pornography, he later admitted that he had been involved in viewing, possessing, and trading child pornography with other users for a period of approximately two years – beginning shortly after he purchased his current desktop computer. ROBERTS stated that he utilized the email addresses of daddyjohn777@gmail.com and smoothies555@hushmail.com to send and receive emails containing images and videos of child pornography on numerous occasions. ROBERTS also admitted that he utilized MediaFire as a means to share child pornography files with other users that were too large to email.

d. ROBERTS advised that he maintained his child pornography files in a folder entitled "misc" or "miscellaneous" on the hard drive of a desktop computer in a bedroom of the residence. He further advised that he categorized the files into multiple sub-folders. ROBERTS installed a password application on the folder(s) to ensure that others in the residence could not view or otherwise access the files.

e. ROBERTS identified that he had access to and utilized a computer in the business office of a Hampton Inn location, where he was employed as a maintenance worker.

56. Computer media seized pursuant to the search warrant were submitted to the Miami Valley Regional Computer Forensics Laboratory (MVRCFL) for analysis. A preliminary examination has been conducted of the desktop computer that ROBERTS identified as being where he maintained his child pornography. To-date, over 3,000 images and over 700 videos of child pornography have been located on this computer. As described by ROBERTS, the files were saved in multiple sub-folders contained within a folder entitled "misc" on the computer's hard drive.

57. Subsequent to the execution of the search warrant at ROBERTS' residence, it was determined that ROBERTS worked at two Hampton Inn locations, one of which was located at 8960 Mall Ring Road in Dayton, Ohio. Management from this Hampton Inn identified that ROBERTS maintained a personal computer in a maintenance room of the hotel. On April 7, 2014, management turned this computer over to the Federal Bureau of Investigation. The computer was identified as being a generic brand desktop computer with the number 02104159 I-501 ATX2 on the back of it. The computer was secured in the Evidence Control Room of the Federal Bureau of Investigation and has not been further examined.

58. As noted above in paragraph 39, ROBERTS sent an email on November 6, 2013 from the daddyjohn777@gmail.com account to another individual with whom he traded child pornography. In the body of the email message, ROBERTS indicated that he was utilizing a computer at his place of employment to send the message. Therefore, it is reasonable to believe that ROBERTS utilized the generic brand desktop computer previously located at the Hampton Inn to send and receive emails to / from those with whom he traded child pornography.

59. Also as noted above in paragraph 39, ROBERTS indicated in the email message that he did not maintain his child pornography files on his work computer. However, by having access to his email account from the work computer computer, he had the ability to access the child pornography files attached to email messages in his inbox and his sent folder. Based on my training and experience, I know that depending on the way the email messages and attached files were opened and viewed on the computer, examiners may have the ability to recover these items during a forensic examination of the computer utilized.

60. Again based on my training and experience, I know that it is common for individuals involved in viewing and possessing child pornography to view and possess files on multiple computers devices. Viewing of child pornography often becomes addictive in nature to such individuals, and they therefore utilize computer devices at multiple locations that they frequent – including at their residences and work locations. Although ROBERTS indicated that he did not maintain his child pornography files on his work computer as of November 6, 2013, it is reasonable to believe that he later saved files onto the work computer to view and/or trade with others.

61. Also subsequent to the execution of the search warrant at ROBERTS' residence, one of the adult females residing at the residence reported that she found two VHS tapes in ROBERTS' bedroom when cleaning the residence. This adult female reported that one of the tapes was in the VCR player of a television and the other tape was under a pile of ROBERTS' clothing. As such, it appears that the tapes were inadvertently overlooked by those executing the search warrant. The adult female did not view the contents of the VHS tapes but rather turned them over to the Federal Bureau Of Investigation on April 16, 2014. The two VHS tapes do not have any labels on them and appear to be non-commercial tapes. The two items were secured in the Evidence Control Room of the Federal Bureau of Investigation and have not been futher examined.

62. Based on my training and experience, I know that VHS tapes are sometimes used by individuals involved in child pornography offenses to store files. In addition, VHS are sometimes used as a means to produce child pornography, and these producers may trade or exchange the tapes with other individuals.

63. Based on the information noted above, I submit that it is reasonable to believe that ROBERTS is the user of the email account daddyjohn777@gmail.com. I further submit that it is reasonable to believe that ROBERTS utilized this and at least one other email account, along with his MediaFire account, to distribute, receive, and possess child pornography.

64. Based on the information noted above, there is probable to believe that evidence of the following violations are contained in the **SUBJECT COMPUTER MEDIA**: (1) possession of child pornography, in violation of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2); and (2) receipt and distribution of child pornography, in violation of Title 18, United States Code, Section 2252(a)(2).

CONCLUSION

65. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. §§ 2252, 2252A, and 2422.

66. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Andrea R Kinzig

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 21st of April 2014

MICHAEL R. MERZ
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO